

REMARKS/ARGUMENTS

The Applicant would like to acknowledge, with thanks, the Office Action that was mailed on February 1, 2007. This amendment is responsive to the February 1, 2007 Office Action. Accordingly, independent claims 1 and 17, and depend claims 5 and 14 have been amended, claims 13, 22-23 have been canceled, and claims 24-26 are new. The subject matter establishing a secure tunnel between the first party and the second party and mutually deriving a tunnel key using symmetric cryptography based on the shared secret is not new matter as it is described in paragraphs 78, 128 and 142 (the paragraph numbers referring to the publication of this application – 2005/0120213) of the original application. Reconsideration of the application as currently amended is now requested.

Claims 22-23 stand rejected under 35 U.S.C. § 101 for including non-statutory matter. Withdrawal of this rejection is requested as these claims have been canceled.

Claims 1-6, 9, 10, and 12-21 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Funk (PAUL; FUNK; Simon Blake Wilson; “draft-ietf-pppext-eap-ttls-02.txt: EAP Tunnelle3d TLS Authentication Protocol (EAP-TTLS)”); Internet-Draft PPPEXT Working Group 30 Nov. 2002, pp. 1-40. Withdrawal of this rejection is requested for reasons that will now be set forth.

Independent claims 1, 17, and 24 recite a method (or an apparatus capable of implementing the method) that comprises provisioning (providing) a party (or an apparatus, such as a wireless device) with a shared secret. A tunnel is established between the first and second parties using the shared secret to mutually derive tunnel keys using symmetric cryptography. An authentication is performed within the secure tunnel.

By contrast, Funk uses asymmetric cryptography to establish the tunnel. Symmetric cryptography is based on the use of a “pre-shared secret” whereby both parties obtain the secret through some protected external means (*see* specification ¶ 3). On the other hand, asymmetric cryptography is based on newer technologies such as “Public Key Infrastructure (PKI) which can enable a “zero knowledge” approach as proof of identification (specification ¶ 4). While asymmetric cryptography can provide a higher level of security than possible with symmetric cryptography, asymmetric cryptography must rely on a third party (known as a Certificate Authority) or must rely on some a priori knowledge to validate the authenticity of the public key.

Funk discloses that EAP-TTLS negotiation comprises two phases: the TLS handshake phase and the TLS tunnel phase (Funk, page 11 § 6). During phase 1, TLS is used to authenticate the TTLS

server to the client and, optionally, the client to the TTLS server (*Id.*). Phase 1 results in the activation of a cipher suite, allowing phase 2 to proceed securely using the TLS record layer (*Id.*). During phase 2, the TLS record layer is used to tunnel information between the client and TTLS server to perform any number of functions such as user authentication, negotiation of data communication security capabilities, key distribution, etc (Page 7 § 6).

However, phase 1 of Funk employs asymmetric cryptography. Funk discloses:

As part of the TLS handshake protocol, the TTLS server will send its certificate along with a chain of certificates leading to the certificate of a trusted CA. The client will need to be configured with the certificate of the trusted CA in order to perform the authentication.

If certificate-based authentication of the client is desired, the client must have been issued a certificate and must have the private key associated with that certificate.

(Page 13 § 6.1). Public-key cryptography, certificates, and the associated PKI are used in EAP-TTLS to authenticate the EAP-TTLS server to the client, and optionally the client to the EAP-TTLS server (page 28 § 12). Thus, Funk discloses using asymmetric cryptography for establishing the tunnel and tunnel key, whereas claims 1, 17 and 24 recite using symmetric cryptography employing the shared secret to establish the tunnel and tunnel key. Therefore, for the reasons just set forth, Funk does not teach or suggest all of the elements of independent claims 1, 17 and 24.

Claims 2-6, 9, 10, and 12-16 directly depend from claim 1 and therefore contain each and every element of claim 1. Claims 18-21 directly depend from claim 17 and therefore contain each and every element of claim 17. Claims 25-26 directly depend from claim 24 and therefore contain each and every element of claim 24. Therefore, for the reasons just set forth for claims 1, 17 and 24, Funk does not teach or suggest all of the elements of claims 2-6, 18-21 and 25-26.

Claims 5-11, 20, 22 and 23 stand rejected under 35 U.S.C. § 103 as being obvious in view of the combination of Funk and Schneier (Schneier, Bruce, "Applied Cryptography", second edition, 1996, pp. 151-157 and 566-571). Claims 22-23 have been canceled. For reasons that will now be set forth, claims 5-11 and 20 are not obvious in view of the combination of Funk and Schneier.

As noted herein *supra*, Funk does not teach or suggest all of the elements of independent claims 1, 17 and 24. The aforementioned deficiency in Funk is not remedied by any teaching of Schneier. In fact, Schneier describes Kerberos, a popular and well known asymmetric cryptographic product. The examiner relies on Schneier to disclose that the first secure credential is a protected access credential (e.g. Kerberos) that can include a protected access credential key which can be a

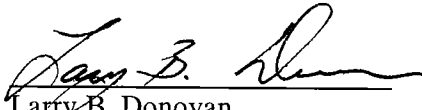
strong entropy key and may include a protected access credential opaque element. None of these teachings of Schneier remedy the aforementioned deficiency in Funk. Therefore, neither Funk nor Schneier, when taken alone or in combination, teach or suggest all of the elements of claims 1, 17 and 24.

Claims 5-11 directly depend from claim 1 and therefore contain each and every element of claim 1. Therefore, for reasons already set forth for claim 1, claims 5-11 are not obvious in view of Funk and/or Schneier when taken alone or in combination. Claim 20 directly depends from claim 17 and therefore contains each and every element of claim 17, therefore, for reasons already set forth for claim 17, claim 20 is not obvious in view of Funk and/or Schneier when taken alone or in combination. Claims 25-26 directly depend from claim 24 and therefore contain each and every element of claim 24. Thus, for the reasons already set forth for claim 24, claims 25-26 are not obvious in view of Funk and/or Schneier.

For reasons just set forth, the claims as currently amended are not anticipated nor obvious in view of the cited prior art and a Notice of Allowance is earnestly solicited. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00010.

Respectfully submitted,

Date: March 6, 2007


Larry B. Donovan
Registration No. 47,230
TUCKER ELLIS & WEST LLP
1150 Huntington Bldg.
925 Euclid Ave.
Cleveland, Ohio 44115-1414
Customer No.: 23380
Tel.: (216) 696-3864
Fax: (216) 592-5009